Introduction to the test data

- Two datasets; orders and HTTP access logs
- The access logs come from nginx
- Mapped according to ECS to not be nginx specific
    - This was handled by our index template

Kibana and the `nested` datatype

- Kibana has limited support for the `nested` datatype
- Full support is a highly requested feature
- On the roadmap, but won't be added anytime soon
- Without it, we would get incorrect results in some scenarios
- Remapping documents might not be feasible
- `nested` fields *can* be used, but there is limited visualization support
- Our documents don't use `nested` fields for these reasons